Vereinbarung zur Auftragsverarbeitung

Als Anlage zum Hauptvertrag
[*genaue Bezeichnung des Hauptvertrags*]
vom [*Datum*]

- nachfolgend „Leistungsvereinbarung“ -

zwischen dem
Deutschen Zentrum für Integrations- und Migrationsforschung e.V. (DeZIM e.V.)
Mauerstrasse 76
10117 Berlin

- nachfolgend „Verantwortlicher“ -

und

[*Vertragspartner: Angabe von Name und Adresse*]

- nachfolgend „Auftragsverarbeitende*r“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

§ 1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf die Verarbeitung personenbezogener Daten entsprechend der Definitionen in Art. 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG - Datenschutz-Grundverordnung (DSG-VO), die Gegenstand der o.g. Leistungsvereinbarung sind bzw. im Rahmen von deren Durchführung verarbeitet oder dem Auftragsverarbeiter bekannt werden.

Nicht unter den Anwendungsbereich fallen Daten von Mitarbeiterinnen und Mitarbeitern des Auftragsverarbeiters, soweit diese ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

§ 2 Konkretisierung des Auftragsinhalts

(1) Gegenstand und Dauer der Auftragsverarbeitung sowie Zweck, Art und Umfang der bestimmen sich nach der o.g. Leistungsvereinbarung.

(2) Folgende Datenarten oder -kategorien sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter:

[genaue Aufzählung oder Beschreibung der personenbezogenen Datenarten oder –kategorien, z.B. Personaldaten, Kommunikationsdaten etc.]. Nicht exemplarisch.

(3) Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen ist

[bitte konkret benennen]

§ 3 Verantwortlichkeit und Weisungsbefugnis

(1) Die Vertragsparteien sind für die Umsetzung der datenschutzrechtlichen Bestimmungen verantwortlich. Der Verantwortliche kann jederzeit den Zugang bzw. die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen in angemessener und wirksamer Weise, insbesondere durch die Anwendung geeigneter technischer und organisatorischer Maßnahmen.

(3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(4) Der Auftragsverarbeiter darf die Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 Buchstabe a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete Anordnung des Verantwortlichen. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

Alle Weisungen erfolgen

☐ schriftlich
☐ per Fax
☐ in Textform/per E-Mail

und sind zu dokumentieren.

(5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Auffassung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. [Die weisungsberechtigten Personen auf Seiten des Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind in Anlage xxx festgelegt.]

(6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.

(7) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(8) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet *der Bundesrepublik Deutschland / der Europäischen* Union *[nicht zutreffende Alternative bitte streichen]* statt.

Eine Verarbeitung in einem Staat außerhalb des in Satz 1 genannten Territoriums ist nur zulässig soweit sichergestellt ist, dass unter Berücksichtigung der Voraussetzungen des Kapitels V der DSGVO das durch die DSGVO gewährleistete Schutzniveau nicht unterlaufen wird und bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

(9) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu den Daten im Rahmen dieses Auftrags haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Eine Verarbeitung der Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, mobiles Arbeiten, Home Office) bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter stellt sicher, dass die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Prinzipien der Datenverarbeitung nach Art. 5 DSGVO einschließlich der Anwendung von erforderlichen bzw. geeigneten technischen und organisatorischen Maßnahmen im Sinne von Art. 24 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

(3) Der Auftragsverarbeiter hat eine/n Datenschutzbeauftragte/n zu benennen, deren/dessen Tätigkeit den rechtlichen Vorschriften entspricht. Die Kontaktdaten der/des Datenschutzbeauftragten sind dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder soweit eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem Anhang „technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang ist Gegenstand dieser Vereinbarung.
Bitte den Anhang im Entwurf vom Auftragnehmer zur Prüfung vorlegen lassen und anschließend abstimmen, ggf. IT-Sachverständige einbeziehen.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der rechtlichen Vorgaben erforderlich sind. Er wird insbesondere Kontrollen und Überprüfungen, die vom Verantwortlichen oder einer anderen vom Verantwortlichen hierzu beauftragten Person oder Steller durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(4) Der Verantwortliche kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der rechtlichen Vorgaben oder der zur Durchführung dieser Vereinbarung erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

(5) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

(6) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherheit der Datenverarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für betroffene Personen zu ergreifen.

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gegen geltende Datenschutzbestimmungen, bei Verstößen gegen diese Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder

34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

§ 7 Löschung und Rückgabe von Daten

(1) Dem Auftragsverarbeiter vom Verantwortlichen überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Ablauf der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen bzw. zu übermitteln oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu vernichten. Der Auftragsverarbeiter stellt dabei sicher, dass ihm, eventuellen Subunternehmern oder einem Dritten keine der von diesem Vertrag betroffenen Daten nach Beendigung des Auftrags mehr zugänglich sind. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Unterauftragsverhältnisse

(1) Der Abschluss von Unterauftragsverhältnissen ist nicht zulässig.

Alternativ kann das Folgende geregelt werden. Allerdings ist eine Vereinbarung, die den Einsatz von Subunternehmen zulässt, stets sorgfältig zu prüfen. Dabei muss die Kapazität und Kompetenz des Verantwortlichen, den Einsatz von Subunternehmern beim Auftragsverarbeiter und die sich daraus steigernde Komplexität des Auftragsverhältnisses bewältigen zu können, als Prüfkriterium berücksichtigt werden. Im Zweifelsfall sollte diese Möglichkeit ausgeschlossen werden:

(2) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmer) nur mit vorheriger ausdrücklicher schriftlicher Zustimmung des Verantwortlichen in Anspruch nehmen. [Die zur Erfüllung dieses Vertrages hinzugezogenen Subunternehmen sind in der Anlage x im Einzelnen bezeichnet. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden]. Sofern es sich um eine allgemeine schriftliche Genehmigung handelt, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmen. Der Verantwortliche kann gegen diese Änderungen Einspruch erheben. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und rechtlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

(4) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortlichen berechtigt, auf schriftliche Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.

(5) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 9 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragen des Verantwortlichen zur Erfüllung ihrer/seiner Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren. Der Auftragsverarbeiter unterwirft sich zusätzlich zu der für ihn bestehenden gesetzlichen Datenschutzaufsicht der Kontrolle der für den Verantwortlichen zuständigen Aufsichtsbehörde für den Datenschutz mit Ausnahme der Bereiche, die keinerlei Bezug zur Auftragserfüllung haben. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte der in Satz 1 und 2 Genannten einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiterinnen und Mitarbeiter anweisen, mit den Genannten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich von Zusicherungen des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommen zu der Bestimmung, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Regelung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Für das Deutsche Zentrum für Integrations- und Migrationsforschung (DeZIM) e.V.

Berlin,	Berlin,
_____	_____
Prof. Dr. Naika Foroutan	Prof. Dr. Frank Kalter
Direktorin DeZIM	Direktor DeZIM
- Dienststempel -	- Dienststempel -

Für *Vertragspartner: Angabe von Name*

Ort,

_____

Titel, Name, Vorname

Dienstliche Stellung im Unternehmen

1

- Dienststempel -

Anhang „Technisch-organisatorische Maßnahmen“

zur Vereinbarung zur Auftragsverarbeitung vom [*Datum*]
zwischen *XXXXX XXXX*
und [*Vertragspartner*]

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den rechtlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter wird seine innere Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Anforderung	Maßnahmen zur Umsetzung der Anforderungen
1.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	*[beschreiben, welche Maßnahmen konkret angewendet werden, um zu verhindern, dass Unbefugte Zutritt erhalten]*[1]
2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	*[beschreiben, welchen Maßnahmen konkret angewendet werden, um zu verhindern, dass die Systeme von Unbefugten genutzt werden]*[2]

[1] Beispiele: Anwendung automatischer Zugangskontrollsysteme, Einsatz von Chipkarten oder Transponder, Kontrolle des Zutritts durch Pförtnerdienste oder Alarmanlagen, Schutz der Serveranlagen in speziell gesicherten Räumen und/oder verschließbaren Serverschränken, konkrete Anweisungen für das Verschließen von Büroräumen, Umgang mit Besuchern, Dienstleistungspersonal, Umgang bei mobiler Arbeit etc

[2] Beispiele: Spezielle Benutzerkennung durch Passwort, Einsatz von Chipkarten zur Anmeldung, konkrete Anweisungen z.B. hausinterne Richtlinien etc.

3.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	*[beschreiben, welche Maßnahmen konkret angewendet werden, um sicherzustellen, dass ausschließlich Berechtigte Zugriff zu haben und eine Verarbeitung durch Unbefugte ausgeschlossen ist]*[3]
	Trennungskontrolle Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	*[beschreiben, welche Maßnahmen angewendet werden]*[4]
4.	**Weitergabekontrolle/Gewährleistung von Vertraulichkeit** Es ist zu gewährleisten, dass personenbezogene Daten bei ihrer Übermittlung an Empfänger nicht unbefugt verarbeitet werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung pb Daten zur Datenübertragung vorgesehen ist.	*[beschreiben, welche Maßnahmen angewendet werden]*[5]
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem pb Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	*[beschreiben, welche Maßnahmen zum Zwecke dieser Kontrolle angewendet werden]*[6]
6.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	*[beschreiben, welche Maßnahmen angewendet werden]*[7]

[3] Beispiele: Pseudonymisierung der pb Daten, Ordnungsgemäße Vernichtung von Datenträgern und Protokollierung, physische Löschung von Datenträgern vor Wiederverwendung, Protokollierung von Vernichtung von IT-Systemen, Installierung von Firewalls, Antivirensystemen, Rechtevergabe + differenziertes Rollen-Rechte-Konzept, Verwaltung des Rechtekonzepts durch Systemadministratoren, keine Nutzung privater Datenträger und privater Endgeräte, 4-Augen-Prinzip, Aufbewahrung von Datenträgern in verschließbaren Schränken/Räumen

[4] Beispiele: Speicherung auf getrennten Systemen (Verwendung verschiedener Server), logische Mandantentrennung softwareseitig, Vergabe von unterschiedlichen Berechtigungen entsprechend der Verfahren

[5] Beispiele: Einsatz von Verschlüsselungsverfahren, gesichertes W-Lan, Nutzung von elektronischen Signaturverfahren, sichere Transportbehältnisse, Dokumentation der Empfänger und Zeitspannen der gelnanten Überlassung von Daten, Weitergabe in Verschlussmappen

[6] Beispiele: technische Protokollierung (Logdateien), Zugriff auf Logdateien nur durch berechtigtes Personal, Kontrolle der Protokolle, Vergabe von Rechten zur Verarbeitung der Daten, klare Regelung zu Aufbewahrungsfristen, klare Zuständigkeiten für Löschungen, nachvollziehbares Dokumentenmanagement

[7] Beispiele: Patch- und Updatemanagement, Backup-Systeme, Firewalls, Brandmeldeanlagen/Rauchmelder, Überspannungsschutz, Klimaanlage in Serverräumen, Feuerlöscher in Serverräumen, Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Raum, regelmäßige Tests zur Datenwiederherstellung und Protokollierung, keine sanitären Anschlüsse im oder nahe des Serverraums

7.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	*[beschreiben, welche Maßnahmen angewendet werden]*[8]

(2) Es ist ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht.[9]

Für das Deutsche Zentrum für Integrations- und Migrationsforschung (DeZIM) e.V.

Berlin,

_____

Prof. Dr. Naika Foroutan

Direktorin DeZIM

- Dienststempel -

Berlin,

_____

Prof. Dr. Frank Kalter

Direktor DeZIM

- Dienststempel -

Für *Vertragspartner: Angabe von Name*

Ort,

_____

Titel, Name, Vorname

Dienstliche Stellung im Unternehmen

- Dienststempel -

[8] Beispiele: Abschluss klarer und unmissverständlicher Vereinbarung mit Dienstleister (AV), sorgfältige Auswahl von Dienstleistern, laufende Überprüfung des Dienstleisters

[9] Softwarelösungen für Datenschutz-Management, Sicherheitszertifizierung, anderweitig dokumentiertes Sicherheitskonzept, Benennung eines/einer Datenschutzbeauftragten